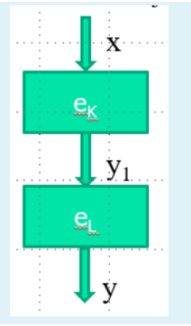
# Prvi kolokvijum iz zaštite sistema

1. **Kod jednokratne bilježnice koristi se:**
   - **Binarni sistem**
2. **Multiplikativni inverz broja a:**
   - **$a^{-1}$ a mod 26 = 1**
3. **Sabrati dva polinoma u AES sistemima 100 i 1010 :**
   - **1110**
4. **Sabrati dva polinoma u AES sistemima 101 i 1010 :**
   - **1111**
5. **Ako je niz 110001b ulaz u supstitucisku kutiju S3 DES algoritma,izlaz je:**
   - **0100**
6. **Ako je niz 101100b ulaz u supstitucisku kutiju S3 DES algoritma,izlaz je:**
   - **0011**
7. **Redosled runda RIJNDAEL-a je:**
   - **ByteSub – ShiftRow – MixColumn – AddRoundKey**
8. **Izlaz L4 se računa kao:**
   - **L4=R3**
9. **AES blokovi predstavljaju matrice:**
   - **4x4 bajta**
10. **Šifre i definicije :**
    - **Cezarova -- monoalfabecka**
    - **Playfair -- bigramska**
    - **Vignerova -- polialfabecka**
    - **Hillova -- poligramska**
    - **Viženerova -- polialfabecka**
    - **Alfina – monoalfabecka**
11. **Indeks koincidencije:**
    - **Index koincidencije ic(x) niza x od n slova definiše se kao vjerovatnoća da su dva slučaja elemenata iz x jednaka**
12. **Međusovni index koincidencije služi za određivanje:**
    - **Ključa**
13. **Shodno dvostukom AES može se napisati:**




    - **$Y=e_L(e_K(x))$**

**14. Formule i nazivi šifri:**

**Vižner - šifrovanje**

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

**Cezarova šifra – dešifrovanje**

$$d_K(y) = y - K \bmod 26$$

**Cezarova šifra – šifrovanje**

$$y = e_K(x) = x + K \bmod 26$$

**Alfina šifra - dešifrovanje**

$$d_K(y) = a^{-1}(y - b) \bmod 26$$

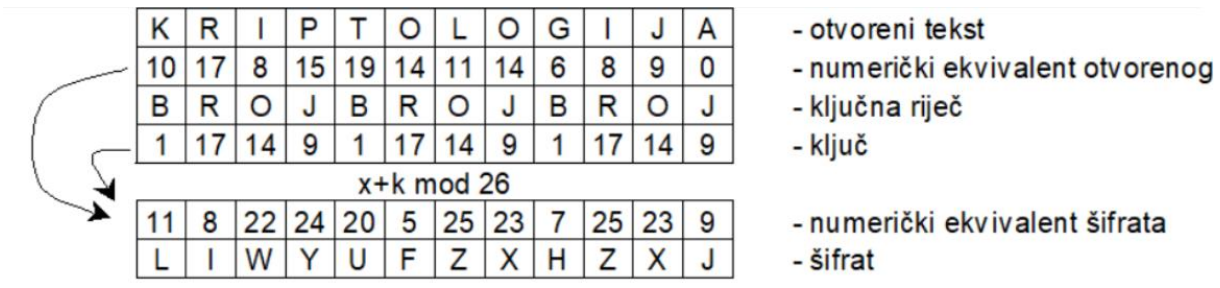
**Alfina šifra - šifrovanje**

$$e_K(x) = ax + b \bmod 26$$

**Vižner - dešiifrovanje**

$$d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

**15. Dat je primjer šifrovanja:**




- **Vigener**

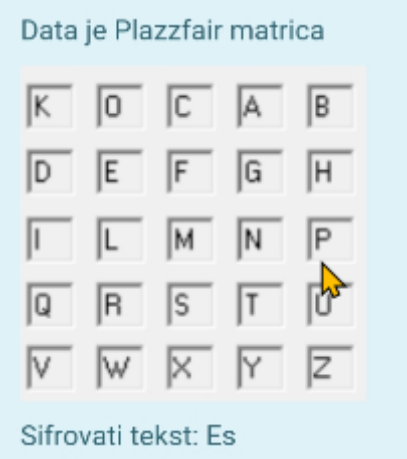
**16. Polinomu $x^6 + x^4 + x^2 + x + 1$ :**

- **01010111**

**17. U AES-u se prilikom sabiranja dva polinoma $x^6 + x^4 + x^2 + x + 1$ i $x^6 + x^4 + x + 1$ dobija:**

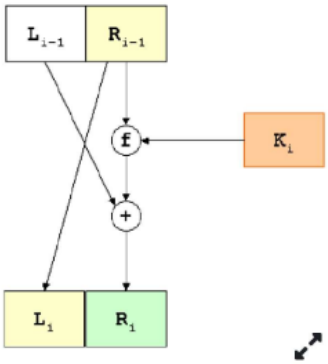
- **100**

18. **Primjenom kaskijevog teksta uočeni su identični segmenti sifrata čije se početne pozicije nalaze na udaljenostima d1=14 d2=49 d3=77 dužina ključa je:**
    - **7**
19. **Primjenom kaskijevog teksta uočeni su identični segmenti sifrata čije se početne pozicije nalaze na udaljenostima d1=20 d2=55 d3=100 dužina ključa je:**
    - **5**
20. **Dužina ključa u DES kriptosistemu (u bitu) sa i bez peritetnih bitova:**
    - **64-56**
21. **Lavinski efekat kod DES-a :**
    - **Mala promjena u ključu izaziva velike promjene u šifratu**
22. **Data je Plazzfair matrica, šifrovati tekst ES:**




    - **FR**

23. **Data je Plazzfair matrica, šifrovati tekst EG:**
    - **FH**
24. **Cezarova šifra: Otvoren tekst F i ključ 23 , šifrat će biti:**
    - **C**
25. **Kod MixColumn obavlja se operacija:**
    - **Množenje polinoma**
26. **Kaskijev tekst služi za određivanje:**
    - **Dužine ključne riječi**
27. **Kod DES algoritma ukupno ima:**
    - **16 rundi**
28. **Kod ByteSub bajt $21_h$ zamjenjuje se bajtom:**
    - **Fd**
29. **Povezati definicije:**
    - **Kriptografski algoritam – matematička funkcija koja se koristi za šifrovanje i dešifrovanje**
    - **Kriproanaliza – naučna disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa**
    - **Kriptologija – naučna disciplina koja obuhvata kriptografiju i kriptoanalizu**
30. **Shodno algoritmu DES-a :**




- **$R_i = L_{i-1}$ ekskluzivno ILI sa f ( $R_{i-1}$ , $K_i$ )**

31. **Ako kriptosistem radi u ECB modu , šifrovanjem ulaznih podataka (djelova otvorenog teksta) x1 , x2 i x3 dobijaju se redom djelovi šifrata y1 , y2 i y3. Šta sve (od x1 , x2 i x3) direktno ili indirektno utiče na vrijednost y3:**
    - **$X_3$**
32. **AddRoundKey predstavlja operaciju :**
    - **XOR AES-BLOKA**
33. **Ako je ključna riječ PLAYFAIT kod istoimene šifre, otvoren tekst ST se šifruje u:**

| | | | | |
|---|---|---|---|---|
| P | L | A | Y | F |
| IJ | R | B | C | D |
| E | G | H | K | M |
| N | O | Q | S | T |
| U | V | W | X | Z |

    - **TN**
34. **Ako je ključna riječ PLAYFAIT kod istoimene šifre, otvoren tekst HZ se šifruje u:**
    - **MW**
35. **Ako je ključna riječ PLAYFAIT kod istoimene šifre, otvoren tekst RG se šifruje u:**
    - **GO**
36. **Dat je primjer šifrovanja/dešifrovanja, odaberi o kojoj se šifri radi :**


    - **Vigner dešifrovanje sa autoključem**
37. **Ako je otvoren tekst A , a ključ (a,b)=(3,1) tada je šifrat prema Alfini:**
    - **E (x) = ax+b mod 26 = (3*0+1)mod 26 = 1 tj. A**
38. **Funkcija f kod DES-a ima oblik f( $R_{i-1}$ , $K_i$ ) = P(S(E($R_{i-1}$)) gdje P predstavlja:**
    - **Permutacije**
39. **Funkcija f kod DES-a ima oblik f( $R_{i-1}$ , $K_i$ ) = P(S(E($R_{i-1}$)) gdje S predstavlja:**

- **Supstituciju**

**40. U AES-u se prilikom sabiranja dva polinoma $x^3+x^3$ dobija se:**

- **0**

**41. Kriptosistem je uređena petorka (P,C,K,E,D) za koji važi:**

- **C je konačan skup svih mogućih šifrata**
- **K je prostor ključeva(svih mogućih ključeva)**
- **P je konačan skup svih mogućih otvorenih tekstova**

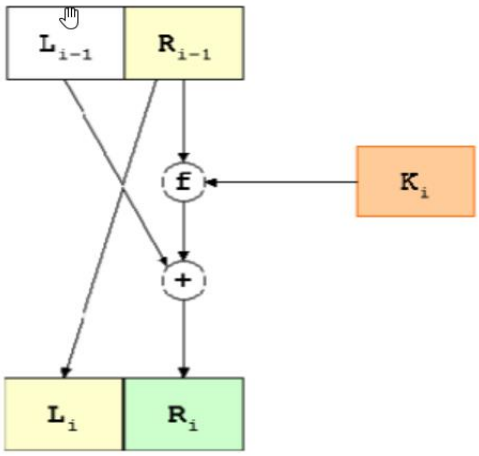
**42. Spoiti odgovvjuće fraze:**

- **ECB svaki blok otvorenog teksta šifruje se se pomoću istog ključa**
- **CBC indetičnim blokovima u otvorenom tekstu odgovaraju različiti šifrati**
- **CFB Prilikom šifrovanja prvo se šifruje 64 bitni inicijalni vektor VI**

**43. Poveži tačne odgovore:**

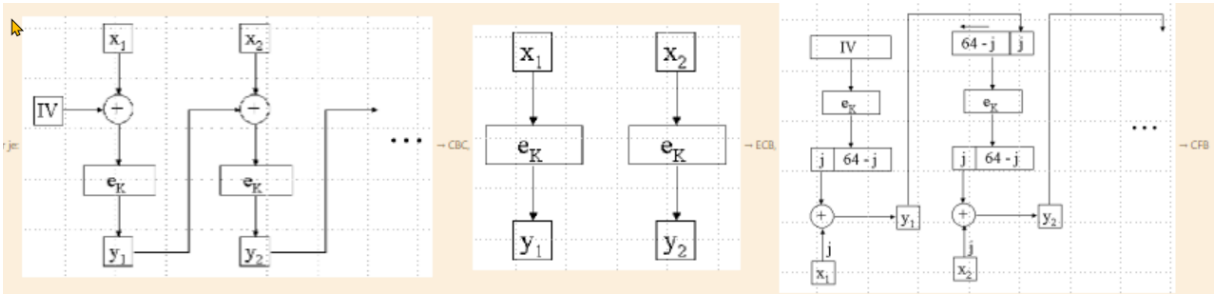
- **Monoalfabecki kriptosistemi -- svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata**
- **Polialfabecki kriptosistemi – slovo otvorenog teskta može se preslikati u jedno od m mogućih slova**

**44. Shodno algoritmu DES-a izaberi jedan odgovor:**




- **$L_i = R_{i-1}$**

**45. SLIKE CBC , ECB , CFB**




**CBC** **ECB** **CFB**

**46. Specifičnost RIJANDEL-a jeste u tome što radi u polju:**

- **$2^8$**

**47. Zadaci sa tačnim odgovorima i tvrdnjama(sve tačne tvrdnje i odgovori iz svih zadataka su ovdje)**

- **Svaka s kutija je fiksna 4 x16 matrica čiji su elementi cijeli brojevi između 0 i 15**
- **Simetrični kriptosistemi - ključ za dešifrovanje isti kao za šifrovanje ili se izračunava na osnovu njega**
- **Kriptosistemi sa javnim ključem - ključ za dešifrovanje (tajni) se ne može izračunati iz ključa za šifrovanje (javni)**
- **Supstituciske šifre - šifre u kojima se svaki element otvorenog teksta (bit,slovo,grup bitova ili slova)preslikava u neki drugi elelement**
- **Transpozicione šifre su šifre u kojima se elementi otvorenog teksta permutuju**
- **DES šifruje blokove otvorenog teksta dužine 64 bita, kosristeći ključ K dužine 56 bita**
- **Blok šifre - određuje se jedan po jedan blok elemenata otvorenog teksta**
- **Protočne šifre - elementi otvorenog teksta obrađuju se jedan po jedan**